Kim D. Stephens, P.S., WSBA #11984
Jason T. Dennett, WSBA #30686
Kaleigh N. Boyd, WSBA #52684
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101-3147
T: (206) 682-5600
F: (206) 682-2992
kstephens@tousley.com
jdennett@tousley.com
kboyd@tousley.com

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WASHINGTON

In re: *Whitworth University Data Breach*	Case No. 2:23-cv-00179-SAB **JOINT STATUS REPORT**

Plaintiffs and Defendant Whitworth University certify that the FRCP 26(f) initial conference among counsel took place on February 20, 2024 and hereby submit the following Joint Status Report in accordance with the Court's Notice Setting Scheduling Conference ECF No. 21.

1. Service. Service is complete.

2. Jurisdiction, Venue, and Standing. Plaintiffs' position is that that jurisdiction, venue, and standing are proper.

Whitworth agrees that venue is proper in this judicial district. Whitworth reserves the right to challenge the Court's subject matter jurisdiction under the Class Action Fairness Act, because each of the named plaintiffs are currently alleged to be domiciled in Washington, so there is no minimal diversity with respect to the named plaintiffs. Further, as to standing, Whitworth reserves the right to challenge the named plaintiffs' standing to sue if facts are revealed to show that they have not suffered a sufficient or any concrete injury.

3. Magistrate. The Parties do not consent for this matter to be tried before a magistrate judge.

4. Nature and Basis of the Case.

Plaintiffs: This case arises out of a targeted cyber-attack that allowed a third-party to gain unauthorized access to the computer systems housing sensitive consumer data maintained by Defendant. In the course of its business, Defendant stores and maintains consumers' sensitive and private information, including their Social Security numbers (the "Private Information"). As a result of Defendant's failure to adhere to adequate data security practices, a malicious actor executed a cyberattack that resulted in its access to the Private Information of Plaintiffs and

over 65,000 other consumers across the country (the "Data Breach"). Plaintiffs bring five claims on behalf of themselves and the class: 1) negligence; 2) breach of implied contract; 3) breach of the implied covenant of good faith and fair dealing; 4) unjust enrichment; and 5) violation of the Washington Consumer Protection Act. The Court denied Defendant's Motion to Dismiss on January 23, 2024.

Defendant:

Defendant Whitworth University has answered the complaint and asserted affirmative defenses and avoidances. Whitworth is a private, Christian, residential, liberal arts higher education institution in Spokane Washington. See University's September 20, 2023 response to the Colorado Department of Law's requests about the data breach. ECF No. 16-1 at page 4 of 101, Attach. 1, Appendix A (Resp. to Req. No. 1). The university's mission is to provide its diverse student body an education of the mind and the heart, equipping its graduates to honor God, follow Christ, and serve humanity. This mission is carried out by a community of Christian scholars committed to excellent teaching and to the integration of faith and learning. *Id.* Recognized as one of the top regional colleges and universities in the West, Whitworth has an enrollment of about 2,500 students. *Id.*

Reading the proposed injunction in the consolidated complaint, one might not know that Whitworth had extensive security policies and practices in place

prior to the July 29, 2022 data breach incident. *See* ECF No. 15 at 46-51; *id.* ¶189. Those policies and practices include:

- Maintained Palo Alto 5220 firewalls configured to best practices for primary gateway for all traffic entering and leaving network. This solution contains Antivirus, Anti-Spyware, Vulnerability Protection, URL filtering, and File blocking profiles.
- Maintained F5-BIG IP for SAML2.0 authentication that is integrated with DUO for MFA authentication for off campus access into all apps that are a part of our Single Sign-on environment. ….
- Installed Bitdefender on all PCs and Servers on campus with daily updates to definitions.
- Maintained an update policy for all servers relating to Windows updates and Patch Management.
- Trained staff with a table-top exercise on a cyber breach and worked to attain Business Continuity Plans from departments.
- Maintained and updated the IT security Policy.
- Maintained a contract with a 3rd party vendor for CISO-as-a-service and monthly meetings about IT security.
- Maintained a data breach/cyber liability insurance policy.

ECF No. 16-1 at pages 4-5 (Resp. to Req. No. 3).

Despite these measures and the policies, Whitworth suffered a data breach that did not impact its main depository for student information. ECF No. 16-1 at page 5 (Resp. 10). The majority of the potentially compromised documents were between 1 and 7 years old and consisted of residence housing, course roster, travel expense, and employment data. *Id.* The breach potentially impacted 65,593 individuals. *Id.* at page 7 (Resp. 16). But 31,255 of these potentially impacted persons had merely their student identification and date of birth accessed. *Id.*. However, the investigation revealed the incident for some may have resulted in the exposure of employee, student, or other affiliate personal information including: names, state identification number, passport number, Social Security number and/or health insurance information. *Id.* at page 3 (Resp. 2).

In response to the breach, Whitworth notified its insurer and engaged Tetra Defense (now Artic Wolf) to conduct a forensic investigation of the ransomware attack by LockBit 3.0 and BianLian and to engage in discussions with the threat actor. ECF No. 16-1 at page 6 (Resp. 14). The threat actor agreed to delete an exfiltrated data as part of the ransom payment. *Id.* at page 8 (Resp. 18). After decryption and restoration was complete, Whitworth remediated the breach by wiping and rebuilding systems with enhanced safeguards. *Id.* at pages 5-11 (Resps.

12, 14, 18, 21). Whitworth also retained legal counsel with national firms to report to state agencies and notify potentially affected students and employees. The first wave of notices were sent to 6,612 individuals on October 3, 2022; the second wave was sent to 58,981 on April 28, 2023. *Id.* at pages 10 (Resp. 21). Whitworth offered potentially impacted persons 12 to 24 months of free credit monitoring and identity theft protection through IDS. *Id.* at pages 8-11 (Resps. 18-21).

5. Trial. The Parties prefer for the Court to set trial for January 2026, and anticipate that trial will take approximately 10 days.

6. Anticipated Motions. Plaintiffs anticipate filing a motion for class certification. Defendant anticipates filing a motion for summary judgment or for judgment on the pleadings.

7. Initial Disclosures. The Parties propose exchanging initial disclosures via email to counsel of record no later than April 15, 2024.

8. Discovery Plan.

A. Initial disclosures.

The Parties propose exchanging initial disclosures via email to counsel of record no later than April 15, 2024.

B. Subjects, timing, and potential phasing of discovery.

Plaintiffs' Position: Plaintiffs intend to take discovery regarding the

following: Defendant's data security practices, the cost to implement those data security practices, and the extent to which those security practices have changed since the Data Breach; the root cause(s) of the Data Breach; the number of individuals impacted by the Data Breach, including whether the an individual's data was exfiltrated, as well as a description of the categories of compromised Private Information for each individual; reports of data misuse or identity theft Class Members have experienced related to the Data Breach (including dark web activity and the alleged offer to sell data taken from Defendant); information about how Defendant came into possession of Class Members' data; contracts governing Defendant's collection, use, and storage of data concerning Class Members; and insurance policies under which an insurer may be liable to pay costs associated with the Data Breach, including indemnification arrangements with outside vendors or other third parties.

Plaintiffs do not believe that discovery should be phased, limited, or focused on particular issues.

Defendant's Position: Defendant intends on taking written discovery regarding: (i) Plaintiffs' factual support for each of their respective claims; (ii) information that each Plaintiff provided to Whitworth; (iii) Plaintiffs' damages, if any, including any alleged fraudulent transactions based on the data breach,

impaired credit and any other alleged damages.

Defendant also intends on retaining experts to establish its defenses regarding its network security and its responses to the data breach.

Defendant believes that discovery should be phased as to propounding discovery on the named plaintiffs and deposing the named plaintiffs before permitting and engaging in class discovery.

C. Electronically Stored Information.

Both parties believe that ESI will be involved in this case. The parties will meet and confer regarding use of an ESI Agreement.

D. Privilege issues.

The Parties are not aware of any privilege issues at this time. The parties believe a Rule 502(d) order may be helpful in this case and will meet and confer regarding any other privilege issues as they arise in the case. The Parties anticipate addressing privilege logging in conjunction with their execution of an ESI Agreement.

E. Proposed limitations on discovery.

At this time, the parties do not see the need for any limitations on discovery beyond those established by the Federal Rules of Civil Procedure and the Local Rules.

F. The need for discovery-related orders.

At this time, the Parties do not believe there is a need for any discovery-related orders.

9. Class Certification. Plaintiffs intend to file a motion for class certification. Plaintiffs propose filing their motion for class certification 192 days before trial. The Parties will enter into a confidentiality agreement and will propose a stipulated protective order covering confidential information.

10. Beneficial Interest of a Minor. This case does not involve the beneficial interest claim or a minor or incompetent person that requires the appointment of a Guardian ad litem.

11. Special Procedures. The Parties do not believe there is a need for special procedures at this time.

12. Modification of Standard Procedures. The Parties do not believe there is a need for modification of the standard procedures at this time.

13. Feasibility of Bifurcation. The Parties do not believe bifurcation is feasible.

14. Alternative Dispute Resolution. The Parties are currently discussing alternative dispute resolution and attempting to reach agreement on a mediator. The Parties will jointly inform the Court if they schedule a mediation.

15. Certification to the Supreme Court. The Parties do not believe there are any issues that should be certified to the State Supreme Court at this time.

16. Other Matters. The Parties agree to email service of all pleadings, discovery, and discovery responses in this case.

Dated: March 11, 2024

Respectfully submitted,

TOUSLEY BRAIN STEPHENS PLLC

By: *s/Kaleigh N. Boyd* /

Kim D. Stephens, P.S., WSBA #11984
Jason T. Dennett, WSBA #30686
Kaleigh N. Boyd, WSBA #52684
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101-3147
T: (206) 682-5600
F: (206) 682-2992
kstephens@tousley.com
jdennett@tousley.com
kboyd@tousley.com

Attorneys for Plaintiffs and the Proposed Class

Samuel J. Strauss
TURKE & STRAUSS LLP
613 Williamson St., Ste. 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-2443

Kevin Laukaitis (admitted *pro hac vice)*
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518

San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Bryan L. Bleichner (admitted *pro hac vice)*
Philip J. Krzeski (admitted *pro hac vice*)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
T: (612) 339-7300
F: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Interim Co-Lead Counsel

BUCHALTER

By: */s/David Spellman /*
David Spellman WSBA #15884
1420 Fifth Avenue, Suite 3100
Seattle, WA 98101-1337
T: 206.319.7052
E: dspellman@buchalter.com

Attorneys for Defendant,
Whitworth University

CERTIFICATE OF SERVICE

I hereby certify that on March 11, 2024, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF System, which in turn automatically generated a Notice of Electronic Filing (NEF) to all parties in the case who are registered users of the CM/ECF system. The NEF for the foregoing specifically identifies recipients of electronic notice.

s/Kaleigh N. Boyd /

Kaleigh N. Boyd, WSBA #52684
Attorney for Plaintiffs
Tousley Brain Stephens PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101-3147
T: (206) 682-5600
F: (206) 682-2992
kboyd@tousley.com